STATE OF MONTANA
DEPARTMENT OF CORRECTIONS
POLICY DIRECTIVE

Policy No. DOC 1.9.13	Subject: **OFFENDER ACCESS TO COMPUTERS**
Chapter 1: ADMINISTRATION AND MANAGEMENT	Page 1 of 4 and Attachment
Section 9: Information Systems	Effective Date: Dec. 1, 1996
Signature: /s/ Mike Ferriter, Director	Revision Dates: 12/01/99; 03/08/01; 06/26/02; 04/26/07

I. POLICY

The Department of Corrections allows offenders controlled access to state-owned computers. This access is allowed for training, legal research, educational purposes, and as needed for work that offenders may perform in Department facilities and programs.

II. APPLICABILITY

All divisions, facilities and programs under Department jurisdiction or contract.

III. DEFINITIONS

Administrator – The official, regardless of local title (division or facility administrator, bureau chief, warden, superintendent), ultimately responsible for the division, facility, or program operation and management.

CIO – The Department's Chief Information Officer.

Computer Peripherals – Any equipment that can be attached to a computer. Peripherals include, but are not limited to:

- printers
- scanners
- digital cameras
- removable data storage media such as pen drives, DVD/CD drives, tape drives, and zip drives**.**

Facility **–** Refers to any prison, correctional facility, correctional or training program under Department jurisdiction or contract.

Freestanding Isolated Network – A group of computers networked only to each other. The freestanding isolated network will not have access to outside LANS, WANS, the Internet or Microsoft Outlook.

IBTB – The Information and Business Technology Bureau of the Department of Corrections.

LAN (Local Area Network) – A collection of computers that share resources such as applications, file systems, and printers.

- MDOC LAN – The Department of Corrections Local Area Network
- Offender LAN **–** A LAN for offender use that is not connected to the MDOC LAN

Offender – Any individual in the custody of the Department of Corrections or its contractors.

Password – An alphanumeric combination of characters unique to individual users that allow access to a specific computer, network or computer system.

Portable Electronic Storage Media (Portable Storage) – Includes floppy disks, CDs, DVDs, optical platters, flash memory drives, backup tapes, external hard drives, and other electronic storage media or devices that provide portability or mobility of data.

Server – A computer that serves programs, files, and printing services to other computers on the network.

Stand-Alone Computer – A computer that is not attached to any network.

User ID – Used generically to refer to logon ID, User ID, account, or any other term used to describe a user's rights and privileges on a computer, computer system or network.

VLAN – A network that is created specifically for offender use and is administered by the Department staff.

WAN (Wide Area Network) – The State of Montana Wide Area Network.

IV. DEPARTMENT DIRECTIVES

A. Prohibitions

1. Under no circumstances will facilities allow any offender to:

    - access the internet
    - access e-mail or any other on-line service such as Microsoft Outlook
    - access supervisory or administrative file servers
    - access WANs
    - access MDOC LAN

2. Under no circumstances will facilities allow offenders to save or maintain personal files on a state owned or leased computer.

B. Computer Labeling

1. Each facility will:

    a. conspicuously label all computers and peripherals, which are located in offender-accessible areas, with a laminated card, designating them as either *Offender Use* or *Staff Use Only* to ensure visual identification;
    b. permit offenders to only access computers labeled *Offender Use;*
    c. ensure the laminated card attached to each *Offender Use* computer includes all authorized programs allowed on that specific computer; and
    d. ensure the card is signed and dated by the work area supervisor or IBTB staff.

2. The work area supervisor, or designee, will inspect the *Offender Use* computers at least on a quarterly basis to ensure that they are in compliance with the laminated card specifications and document all inspections in writing.

C. Offender Access to Stand Alone Computers or Free Standing Isolated Networks

1. The work area supervisor may allow an offender to access stand-alone computers and freestanding isolated networks; however, the computers must be labeled as outlined in Section B.

2. The administrator and CIO must approve in writing the creation of any new, free-standing, isolated networks.

D. Offender Access to VLAN

1. The IBTB, in conjunction with the Department of Administration's Information Technology Services Division, will manage the VLAN and its servers.

2. The Department computer security officer and administrator must provide written approval for offender access to VLAN for work that the offender may perform in Department facilities.

3. To request offender access to VLAN, the appropriate supervisor must complete the "Offender Access to DOC Computer VLAN Request Form" (see Attachment A), and submit the form for approval as outlined in item D.2 above.

4. Once an offender is approved for VLAN access, the Department computer security officer will assign the offender the appropriate rights on the file server. The Department computer security officer will send the offender's User ID number and password to the requesting supervisor.

5. Area supervisors will log offenders onto the VLAN. Under no circumstances will supervisors allow offenders to know the password used with his or her User ID.

6. When an offender leaves a job assignment, the work area supervisor must notify the Department computer security officer to remove the offender from VLAN access.

E. Offender Access to Peripherals and Disks

1. Each facility will ensure that offender access to peripherals is limited and closely supervised.

2. Each facility will develop specific procedures regarding the use of all peripherals. In the case of scanners and digital cameras, the supervisor must review and approve the project in writing prior to allowing the offender access to the equipment.

3. Supervisors may allow offenders to use portable electronic storage media for appropriate work-related assignments and educational programs in coordination with the Department computer security officer and area supervisor.

4. Under no circumstances will supervisors allow offenders to move portable electronic storage media from their assigned work area to another area without staff approval.

5. Possession of portable electronic storage media in offender living areas or use of disks for personal needs is strictly prohibited.

V. CLOSING

Questions concerning this policy should be directed to the Department's Chief Information Officer (CIO.)

VI. REFERENCES

A. *2-15-112, MCA (2005) Duties and Powers of Department Heads; 2-15-114, MCA (2005) Security Responsibilities of Departments for Data; 53-1-203, MCA (2005) Powers and Duties of Department of Corrections.*

B. *1-0250.00, Montana Operations Manual*

VII. ATTACHMENT

Offender Access to DOC Computer VLAN Request Form

OFFENDER ACCESS TO DOC COMPUTER VLAN REQUEST FORM

This form will be used for all requests for offender access to the DOC computer Virtual Local Area Network (VLAN). Please complete and route this request form in the order of the following sections.

The following portion to be completed and signed by the work supervisor:

DOC Division: _____

Offender Work Location: _____

Offender Name: _____ AO#: _____

Justification for VLAN request: _____

_____

_____

Work Supervisor Printed Name: _____

Work Supervisor Signature: _____ Date: _____

Program Manager/Director Signature: _____ Date: _____

The following section is to be completed by the appropriate administrator, or designee.

Approved: ☐ Disapproved: ☐ Date: _____

Comments: _____

_____

_____

Printed Name: _____ Signature: _____

The following section to be completed by the DOC Information and Business Technology Bureau:

☐ Approved: ☐ Disapproved: Date: _____

Comments: _____

_____

_____

Printed Name: _____ Signature: _____

Printed Name: _____ Signature: _____

UserID # assigned: _____ Effective Date: _____

Upon completion of all sections above, send copies to originating work location, Facility Security Manager/Major, and DOC Information and Business Technology Bureau (COR Help Desk.)